Cyberangriffe auf KMU nehmen zu

Der aktuelle Fall eines Liechtensteiner KMU, das derzeit mit einer Cyberattacke kämpft, zeigt: Angriffe häufen sich auch hierzulande.

Dorothea Alber

In den letzten Monaten kam es zu mehreren schwerwiegenden Ransomware-Attacken auf Unternehmen und Behörden in der Schweiz – und auch in Liechtenstein. Der Fall der Universität Liechtenstein, die von einer Cyberattacke betroffen war, sollte nicht der Einzige bleiben. Ein KMU im Land ist derzeit zum Warten verdammt. Ein Krimineller hat alle Kundendaten und alle Rechnungen sowie Dokumente der Buchhaltung gestohlen und verschlüsselt. Mit dem Betreff «Ihre Daten wurden verschlüsselt» flattert dann eine E-Mail ins Haus mit einem Text, der keinen Zweifel offen lässt: «Wir haben Sie gehackt.» Der betroffene Betrieb hatte seine Daten konkret in die Hände eines Schweizer Cloud-Anbieters gelegt, der gehackt wurde. Die Erpresser sitzen irgendwo im Verborgenen und fordern Bitcoin als «Lösegeld».

IT-Unternehmen in Liechtenstein warnen: Cyberattacken nehmen auch hierzulande zu. Bild: Keystone

Cyberattacken: Worauf die Angreifer abzielen

Es ist kein Einzelfall. «Die Angriffe haben massiv zugenommen und dieser Trend wird sich fortsetzen», sagt Jörg Augustin von Pro-IT, dem Branchenverband der Sektion Informatik der Wirtschaftskammer Liechtenstein. «Dabei geht es meist um Ransomware-Attacken», sagt der Experte, der mit HSL Informatik selbst ein IT-Unternehmen führt. Auch andere IT-Betriebe im Land bestätigen das Phänomen. «Allgemein sehen wir eine Zunahme von Angriffen auf Unternehmen in Liechtenstein», bestätigt der Sicherheitsexperte Peter Schenk vom Unternehmen «2sic internet solutions» in Triesen. Auch sogenannte Exchange-Attacken waren in den vergangenen Monaten häufig zu beobachten, bei denen es Angreifer auf Microsoft-Exchange-Server abgesehen haben. Bei Ransomware-Attacken sagt Schenk: «Mit guten Produkten und einem intelligenten Virenschutz ist es möglich, Verschlüsselungstrojaner zu blockieren. Da wir solche Produkte verwenden, sind unsere Kunden fast nie von Ransomware-Attacken betroffen.» Einen 100-prozentigen Schutz gibt es Experten zufolge nicht. Allgemein lasse sich laut Schenk beobachten, dass Unternehmen, die von Ransomware-Attacken betroffen sind, meist nicht ausreichend vorbereitet sind. Die weitverbreiteten Mängel im IT-Bereich sind in den Augen von Fachleuten der Grund dafür, warum sich solche Attacken zu einer elementaren Bedrohung für die Wirtschaft entwickeln konnten. Oft werden minimale Sicherheitsstandards nicht eingehalten. «Das Erste, worauf Angreifer abzielen, ist das Back-up eines Betriebes. Wenn es Hackern gelingt, dieses zu verschlüsseln, wird ein Unternehmen erpressbar.» Bei vielen Firmen wird ein Back-up vernachlässigt oder nicht regelmässig überwacht, weshalb eine Verschlüsselung erst zu spät auffällt. Doch wo ist das Einfallstor, das Kriminelle nutzen? «In 90 Prozent der Fälle wird auf einen Link im Mail geklickt, daher ist Sensibilisierung wichtig», sagt Augustin. Oft sind es gefälschte Mails mit vermeintlich vertrauenswürdigem Absender – der Chef zum Beispiel, der um eine Überweisung bittet. Experten raten: Wer glaubt, eine verdächtige Mail geöffnet zu haben, sollte dies sofort melden. Denn auch wenn gemäss Schenk im ersten Moment alles normal wirkt: Sobald das Einfallstor einmal geöffnet ist, beginnt das Ausspähen im Hintergrund, ohne Aufmerksamkeit zu erregen.

Der Trend geht dabei klar in eine Richtung: Cybercrime im engeren Sinne – also Angriffe auf Daten oder Computersysteme – haben sich laut Landespolizei im vergangenen Jahr im Land gegenüber dem Vorjahr verdreifacht. In der Schweiz haben Kriminelle im gleichen Zeitraum die Daten von rund 2700 Schweizer Unternehmen gestohlen und zum Verkauf ins Darknet gestellt. Für den Inhaber des KMU, der von der Attacke betroffen ist, heisst es weiter abwarten.

Massiver Schaden befürchtet

Die Rede ist bereits von einem «immensen Schaden». Auf einmal sind Daten weg, der Zugriff auf künftig fixierte Kundentermine bleibt verwehrt. Der Cloud-Anbieter in der Schweiz will auf die Forderungen der Erpresser eingehen und so hofft der Betrieb im Land auf die Chance, die Daten wiederzubekommen. Falls nicht, gibt es zumindest den kleinen Trost, dass er noch auf ältere Daten in Papierform zurückgreifen kann – vor der Umstellung auf die Cloud. Wie die Verhandlungen mit den Erpressern ausgingen, ist noch nicht bekannt. Es bleibt ein offenes Drama. Ein Pakt mit der dunklen Seite, der vielleicht Erfolg verspricht – und vor dem die Polizei warnt.

Ransomware-Angriff: So läuft die Cyberattacke ab

Bei Ransomware handelt es sich um Schadsoftware, mit welcher Cyberkriminelle ein Computersystem infizieren, um das Opfer zu erpressen. Die Angreifer verschlüsseln die Daten und fordern ein Lösegeld (engl. ransom). Die Attacke erfolgt in drei Stufen: Zuerst dringt der Angreifer – meist über Pishing-Mails – mehr oder weniger zielgerichtet ein. Danach kundschaftet er die Systeme aus. Er kopiert Daten und verschlüsselt dann vor allem das Back-up.

Auch Liechtenstein ist für Sklaverei indirekt mitverantwortlich

Die gestrige Veranstaltung zum Projekt «Initiative on Finance Against Slavery and Trafficking» fand beim Publikum Anklang.

Bis zum Jahr 2030 wollen die Vereinten Nationen die Sklaverei beenden. Dazu hatte Liechtenstein als Beitrag die «Initiative on Finance Against Slavery and Trafficking» – kurz FAST – lanciert. Das Projekt soll den globalen Finanzsektor ins Zentrum der Bekämpfung von moderner Sklaverei und Menschenhandel stellen.

Gestern und heute findet eine Konferenz statt, welche die Überprüfung der Initiative in den Fokus stellt. Die Regierung lud gestern Abend zu einer öffentlichen Veranstaltung in die Universität Liechtenstein ein, in der Referate gehalten und eine Podiumsdiskussion abgehalten wurden.

Die Moderation führte Botschafter Christian Wenaweser. Aussenministerin Dominique Hasler referierte zu Beginn, und an der Podiumsdiskussion beteiligten sich Ursula Finsterwald, Head Sustainability LGT, Hennie Verbeek Kusters, Vorsitzende der Egmont Group of Financial Intelligence Units, Dame Sara Thornton, Anti-Sklaverei-Kommissarin des Vereinigten Königreichs, Daniel Thelesklaf, Projektdirektor der «Liechtenstein Initiative», und Anti-Geldwäschereiexperte Barry Koch, der per Videoübertragung zugeschaltet war. Auch übertragen wurden die eindrücklichen Worte von Timea Nagy Payne, die ein Opfer von Menschenhandel gewesen ist.

Die Geschichte von Timea Nagy Payne traf die Zuhörer. Bild: Julian Konrad

Über 40 Millionen Menschen in der Sklaverei

Noch heute leben über 40 Millionen Menschen in sklavenähnlichen Zuständen. Und Liechtenstein übernimmt Verantwortung, weil Liechtenstein Verantwortung zu übernehmen hat, lautete der Tenor gestern. Wir würden alle als Konsumenten und Produzenten indirekt von der Sklaverei profitieren, sagt Hasler: «Die von uns verwendeten Rohstoffe stammen oftmals aus Ländern, in denen prekäre Arbeitsbedingungen herrschen.» Die finanzielle Komponente spiele daher eine Schlüsselrolle gegen Sklaverei. Das organisierte Verbrechen transferiert seinen Profit aus Sklaverei und Menschenhandel über reguläre Finanzinstitute. Gerade Liechtenstein müsse mit seinem Finanzplatz solche Strukturen unterbinden.

Hasler stellte die konkreten Erfolge vor, die das Projekt bisher erreicht hat. Im Rahmen von FAST wurde ein Zertifikat für Beauftragte der Sorgfaltspflicht ausgearbeitet, das mittlerweile von über 10 000 Finanzexperten abgeschlossen wurde. Zudem wurde dank FAST über 2000 Menschenhandelsopfern ermöglicht, wieder Zugang zu Bankdienstleistungen zu erhalten. Mittlerweile konnten als Partner Norwegen, die Niederlande und Australien gewonnen werden, die auch finanziell die Zukunft des Projekts sichern.

Ehemaliges Opfer von Menschenhandel erzählt

Im Zentrum standen am gestrigen Abend Menschenhandel und die damit zusammenhängende sexuelle Ausbeutung.

Die 44-jährige Timea Nagy Payne, Menschenhandelsopfer und ehemaliges Mitglied der «Liechtenstein Initiative» gewährte persönliche Einblicke in ihre Erfahrungen. Nagy Payne ging mit 21 Jahren von Budapest nach Kanada, um als Kindermädchen zu arbeiten. Dort realisierte sie, dass die Arbeitgeber dem organisierten Verbrechen aus der Ukraine, Italien, Kanada und Ungarn angehörten. «Ich endete drei Monate lang als Sexsklavin in einem Land, dessen Sprache ich nicht konnte», so Nagy Payne. Dank der Hilfe von Einheimischen gelang es ihr, zu entfliehen. Sie reiste zurück nach Ungarn. Die dortige Regierung sei noch nicht bereit gewesen, Überlebenden Gehör zu schenken. Also ging sie zurück nach Kanada, um sich zu verstecken. Nagy Payne sagte: «Das Schlimmste, was uns passiert, ist nicht der Menschenhandel an sich, sondern das, was danach passiert.» Sie versuchte ein Leben aufzubauen, ohne Sprachkenntnisse und ohne richtige Ausweise. In Folge war es ihr nicht möglich, Bankdienstleistungen in Anspruch zu nehmen. Vor zwei Wochen unterschrieb sie erstmals einen Mietvertrag ohne Mitunterschrift.

«Nach all dem, was wir durchgestanden haben, wollen wir einfach nur ein Teil der Gesellschaft sein» resümiert sie.

Damian Becker